

KeyToken User Manual - 20140112

(주)**키페어**

www.keypair.co.kr

[Blank Page]

목	차
---	---

I. KeyToken 소개1
1. KeyToken 개요1
2. KeyToken HSM1
3. KeyToken MSD4
4. KeyToken USB5
5. KeyToken 사용환경6
II. KeyToken 구동 프로그램7
1. 구동 프로그램 다운로드
2. 구동 프로그램 설치8
3. 구동 프로그램 삭제16
III. KeyToken Manager18
1. 공인인증서 복사18
2. 공인인증서 삭제
3. KeyToken 초기화
4. KeyToken 비밀번호 변경31
5. Keypair 홈페이지 연결33
IV. KeyToken 사용하기34
1. 공인인증서 로그인
2. 공인인증서 발급
3. 공인인증서 갱신
V. FAQ

그 림 목 차

그림 1. KeyToken HSM의 앞면과 뒷면	1
그림 2. KeyToken HSM의 구성도	1
그림 3. KeyToken MSD의 앞면과 뒷면	4
그림 4. KeyToken MSD의 구성도	4
그림 5. KeyToken USB의 앞면과 뒷면	5
그림 6. KeyToken USB의 구성도	5
그림 7. 키페어 홈페이지의 다운로드 페이지	7
그림 8. 실행파일 다운로드	8
그림 9. KeyTokenSetup.zip 파일 열기	9
그림 10. KeyTokenSetup.exe 파일 실행하기	9
그림 11. 실행 허용 선택하기	
그림 12. Microsoft .NET Framework 4.0 Client 설치 시작	
그림 13. Microsoft .NET Framework 4.0 Client 다운로드 중	11
그림 14. Microsoft .NET Framework 4.0 Client 설치 중	12
그림 15. KeyToken Manager 설치 시작	
그림 16. KeyToken Manager 설치 진행중	
그림 17. KeyToken 찾기	
그림 18. KeyToken 초기화 정보 입력	
그림 19. KeyToken 초기화 시작	
그림 20. KeyToken 초기화 완료	15
그림 21. KeyToken Manager 설치 완료	
그림 22. KeyToken Manager 삭제 시작	
그림 23. KeyToken Manager 삭제 진행중	

그림 24. KeyToken Manager 삭제 완료	
그림 25. KeyToken Manager 아이콘	19
그림 26. 복사할 공인인증서 선택	19
그림 27. 복사할 위치 선택	20
그림 28. 비밀번호 입력	20
그림 29. 공인인증서 복사	21
그림 30. 공인인증서 복사 완료	21
그림 31. 복사할 공인인증서 선택	22
그림 32. 복사할 위치 선택	22
그림 33. 비밀번호 입력	23
그림 34. 공인인증서 복사	23
그림 35. 공인인증서 복사 완료	24
그림 36. KeyToken App 설치 QR 코드 및 실행 화면	
그림 37. 삭제할 공인인증서 선택	25
그림 38. 공인인증서 삭제	26
그림 39. 공인인증서 삭제 확인	
그림 40. 공인인증서 삭제 재확인	27
그림 41. 공인인증서 삭제 완료	27
그림 42. KeyToken 관리 탭 선택	
그림 43. KeyToken 초기화 정보 입력	29
그림 44. KeyToken 초기화 시작	29
그림 45. KeyToken 초기화 확인	30
그림 46. KeyToken 초기화 재확인	30
그림 47. KeyToken 초기화 완료	

그림 48. KeyToken 비밀번호 입력	
그림 49. KeyToken 비밀번호 변경 시작	32
그림 50.KeyToken 비밀번호 변경 완료	33
그림 51. 키페어 홈페이지 연결	33
그림 52. 은행 홈페이지 접속	34
그림 53. 공인인증서 로그인 시작	35
그림 54. KeyToken 선택	35
그림 55.KeyToken 비밀번호 입력	36
그림 56. 공인인증서 로그인 완료	
그림 57. 증권사에서 KeyToken 처음으로 사용하기	37
그림 58. 윈도우 시작 버튼 누르기	37
그림 59. regedit 실행하기	
그림 60. USE_SMARTCARD 항목 찾기	
그림 61. USE_SMARTCARD 값 데이터 변경하기	39
그림 62. USE_SMARTCARD 값 데이터 변경 확인하기	39

[Blank Page]

I. KeyToken 소개

1. KeyToken 개요

KeyToken은 공인인증서를 안전하게 저장하고 또 안전하게 사용하기 위한 보안 제품으로, 한국인터넷진흥원(KISA)이 KeyToken의 보안토큰에 대한 구현적합성을 평가하고 인증한 제품입니다.

KeyToken 제품은 공인인증서 전용 제품인 KeyToken HSM, microSD 리더기 겸용 제품인 KeyToken MSD, USB 메모리 겸용 제품인 KeyToken USB의 3가지 모델이 있습니다.

2. KeyToken HSM

그림 1의 KeyToken HSM은 그림 2와 같이 보안토큰과 백업영역을 가진 공인인증서 전용 제품입니다.



그림 1. KeyToken HSM의 앞면과 뒷면



그림 2. KeyToken HSM의 구성도

KeyToken의 보안토큰은 물리적 보안 및 암호연산기능을 가진 보안칩 안에서 구현되어, 현재 공인인증서를 저장하고 사용하는 방법들 중에서 가장 안전합니다.

♦ KeyTokne의 보안토큰은 공인인증서가 외부로 유출되지 않아 안전합니다.

이동식 디스크나 하드 디스크에 저장되어 있는 공인인증서는 쉽게 복사될 수 있어, 해킹 등으로 쉽게 유출될 수 있습니다. 하지만, KeyToken의 보안토큰에 저장되어 있는 공인인증서는 보안토큰 내부에서만 사용되며, 이동식 디스크나 하드 디스크로 복사되지 않아서 공인인증서의 외부유출을 원천적으로 방지하여 안전합니다.

- ★ KeyToken의 보안토큰을 사용하여 새로운 공인인증서를 발급받을 수 있습니다. 금융기관 홈페이지에서 KeyToken의 보안토큰을 사용하여 공인인증서를 새로 발급 받으면, 공인인증서의 외부유출이 원천적으로 방지되기 때문에, 공인인증서를 가장 안전하게 사용할 수 있습니다.
- ◆ <u>기존의 공인인증서를 KeyToken의 보안토큰으로 복사하여 사용할 수 있습니다.</u> 이동식 디스크나 하드 디스크에 저장되어 있는 기존의 공인인증서는 KeyToken의 보안토큰으로 복사하여 안전하게 사용할 수 있습니다. 이때 기존의 공인인증서는 KeyToken의 백업영역과 같은 안전한 곳에 백업하여 보관하시기 바랍니다.
- ★ KeyToken의 보안토큰은 최대 6개의 공인인증서를 저장할 수 있습니다.
 KeyToken의 보안토큰은 은행용/증권용/범용/법인용 등 최대 6개의 공인인증서를 저장하여 사용할 수 있습니다.
- ◇ NFC 스마트폰에서 KeyToken의 보안토큰을 사용할 수 있도록 준비 중입니다. KeyToken의 보안토큰은 PC에서 USB로 연결하여 은행, 증권사 등의 홈페이지에서 바로 사용가능하며, NFC 스마트폰에서도 사용할 수 있도록 준비 중입니다. 현재, 스마트폰의 금융앱이 KeyToken의 보안토큰과 NFC로 통신하는 기능을 협의 중에 있으며, 기능이 추가되기 전까지는 KeyToken의 백업영역 기능을 사용하여 현재의 방식보다 안전하게 스마트폰에서 공인인증서를 사용할 수 있습니다.

KeyToken의 백업영역도 물리적 보안 및 암호연산기능을 가진 보안칩 안에서 구현되어, 현재 공인인증서를 백업하는 방법들 중에서 가장 안전합니다.

2

♦ KeyToken의 백업영역은 하나의 공인인증서를 백업할 수 있습니다.

KeyToken의 백업영역은 하나의 공인인증서를 백업하여 보관할 수 있습니다.

☆ KeyToken의 백업영역에 보관중인 공인인증서는 이동식 디스크로 복사할 수 있습 니다.

은행, 증권사, 보험사, 신용카드사, 전자민원, 국세청 등 대부분의 금융 및 공공기관 홈페이지에서 KeyToken의 보안토큰을 사용할 수 있습니다만, 드물게 보안토큰을 지원하지 않는 사이트들이 존재합니다. 이 경우, KeyToken의 백업영역에 보관되어 있는 공인인증서를 이동식 디스크로 복사하여 사용할 수 있습니다.

☆ KeyToken의 백업영역에 보관중인 공인인증서는 NFC 스마트폰으로 복사할 수 있습니다.

KeyToken의 백업영역에 보관되어 있는 공인인증서를 NFC 스마트폰으로 복사하여, 현재의 방식보다 안전하게 공인인증서를 사용할 수 있습니다. 자세한 내용은 'KeyToken App Manual'을 참조하시기 바랍니다.

KeyToken의 보안칩은 자동잠김기능과 초기화기능 등을 제공하여 공인인증서를 안전하게 관리합니다.

♦ KeyToken의 보안칩은 자동잠김기능이 있어, 분실시에도 안전합니다.

KeyToken의 보안칩은 8자이상 16자이하의 비밀번호를 사용합니다. 이 비밀번호가 연속으로 5회이상 틀리면, KeyToken의 보안칩은 자동으로 잠겨서 보안토큰과 백업 영역을 더 이상 사용할 수 없도록 합니다. 타인이 8자이상의 비밀번호를 5회안에 맞추는 것은 확률적으로 거의 불가능하므로, KeyToken을 분실하더라도 KeyToken 안의 공인인증서는 사실상 안전합니다.

☆ KeyToken의 보안칩은 초기화기능이 있어, 본인이 KeyToken 비밀번호를 잊어버린 경우에도 KeyToken 제품은 다시 사용할 수 있습니다.

KeyToken의 보안칩은 본인이 KeyToken 비밀번호를 잊어버린 경우에도 초기화하여 다시 사용할 수 있습니다. 다만, 초기화될 때 KeyToken 비밀번호와 보안토큰, 백업 영역 안의 모든 데이터가 완전히 삭제되므로, KeyToken 비밀번호를 새로 설정해야 하고 공인인증서도 새로 발급받거나 다시 복사해 넣어야 합니다.

fîKeypair

3. KeyToken MSD

그림 3의 KeyToken MSD는 그림 4와 같이 보안토큰, 백업영역, microSD 리더기를 가진 제품입니다.



그림 3. KeyToken MSD의 앞면과 뒷면



그림 4. KeyToken MSD의 구성도

KeyToken MSD에서 보안토큰, 백업영역, 보안칩에 대한 기능은 KeyToken HSM에서의 기능과 동일합니다. KeyToken MSD는 KeyToken HSM과 PC용 microSD 리더기가 결합된 제품입니다. (microSD 메모리는 별매품입니다.)

★ KeyToken MSD에 microSD를 넣은 후 이동식 디스크로 사용할 수 있습니다.
 그림 3의 오른쪽 그림과 같이 KeyToken MSD 뒷면의 뚜껑을 연 후, microSD를
 넣고 뺄 수 있습니다.

☆ <u>사용자가 원하는 성능과 용량의 microSD/SDHC/SDXC를 사용할 수 있습니다.</u>
 KeyToken의 microSD 리더기는 최대 20MB/s의 전송속도와 최대 64GB의 용량을 지원합니다.

4. KeyToken USB

그림 5의 KeyToken USB는 그림 6과 같이 보안토큰, 백업영역, USB 메모리를 가진 제품 입니다.



그림 5. KeyToken USB의 앞면과 뒷면



그림 6. KeyToken USB의 구성도

KeyToken USB에서 보안토큰, 백업영역, 보안칩에 대한 기능은 KeyToken HSM에서의 기능과 동일합니다. KeyToken USB는 KeyToken HSM과 PC용 USB 메모리가 결합된 제품 입니다. KeyToken의 USB 메모리는 8GB의 경우 최대 18MB/s의 쓰기, 최대 20MB/s의 읽기 성능을 가집니다. 용량은 8 / 16 / 32 / 64GB 제품이 있습니다.

※ 키페어는 제품에 저장된 데이터의 손실에 대한 복구나 배상 책임을 지지 않습니다. 데이터가 손실되지 않도록 반드시 백업하면서 사용하시기 바랍니다.

5. KeyToken 사용환경

♦ <u>PC</u>

인터페이스 : USB 1.1 / 2.0

운영체제 : Windows 8 (32/64-bit), Windows 7 (32/64-bit), Windows Vista (32/64-bit), Windows XP (32-bit)

인터페이스 : NFC 운영체제 : 안드로이드 v2.3.6 (진저브레드) 이상

II. KeyToken 구동 프로그램

KeyToken을 PC에서 사용하기 위해서는, 먼저 PC에 구동 프로그램을 설치해야 합니다.

1. 구동 프로그램 다운로드

KeyToken 구동 프로그램은 키페어에서 제공하는 KeyTokenSetup.exe 파일을 실행하면 설치됩니다. KeyTokenSetup.exe 파일은 아래의 방법으로 구할 수 있습니다.

☆ microSD를 내장한 KeyToken MSD 제품 또는 KeyToken USB 제품에는 미리 저장 되어 있습니다.

microSD를 내장한 KeyToken MSD 제품은 microSD에, KeyToken USB 제품은 USB 메모리에, KeyTokenSetup.exe 파일이 미리 저장되어 있습니다.

웹 브라우저에서 아래의 주소를 직접 입력하여 키페어의 홈페이지로 접속한 후, 그림 7과 같이 다운로드 페이지로 이동하여 'KeyToken 구동 프로그램' 설치파일을 다운로드 받을 수 있습니다.

🗲 🔿 🧭 http://www.keypair J	D ~ 물 Ĉ 🦉 Keypair ×	• □ •ו
f®Keypair	•회사소개 •보안 하드웨어 •보안 소프트웨어 •다운로드 •고	1객센터
DOWNLOAD	Information Security Download	
	* Keypair * KeyToken HSM * KeyToken MSD * KeyToken USB * 스마트폰용 앱 며 11일로 문제하는 전 11일 모두보스 세운으로 이용 KeyToken 개용 소기원서 KeyToken 개용 소기원서	suq.
	KeyToken HSM KeyToken 구등 프로그램 KeyToken HSM 무정정 따라하기 KeyToken HSM 무정정 따라하기 KeyToken HSM 주장정 따라하기 KeyToken 사용자 매뉴얼 용서 다운로드 문서 다운로드	2
	ReyToken 전통 프로그램 상사파일 다운로드 (ÿ

http://www.keypair.co.kr

그림 7. 키페어 홈페이지의 다운로드 페이지

2. 구동 프로그램 설치

KeyToken은 PC에서 사용되기 전에, 반드시 PC에 KeyToken 구동 프로그램이 설치되어 있어야 합니다.

이 절에서는 KeyToken HSM에 대한 구동 프로그램을, Windows 7의 Internet Explorer 9로 키페어 홈페이지에서 다운로드 받은 후, 설치하는 과정을 예를 들어서 설명합니다. 기본 적으로 Windows 8, Windows Vista, Windows XP에서도 동일한 과정으로 설치됩니다. 다만, 설치에 앞서 운영체제를 최신 상태로 업데이트하시기를 권장합니다.

 그림 8과 같이 키페어 홈페이지의 다운로드 페이지에서 해당 제품의 '실행파일 다운로드' 버튼을 누릅니다.

A ttp://www.keypair \$	D ~ ≅ C Ø Keypair ×	- □ -×- n * ¤
f îKeypair	· 회사소개 · 보안 하드웨이 · 보안 소프트웨어	•다운로드 ·고객센터
DOWNLOAD	Information Security Download	
	* Keypair * KeyToken HSM * KeyToken MSD * KeyToken H 1913 KeyToken 現職 会現人 KeyToken 現職 会現人 KeyToken, Product_information_20131017.pdf	1 USB * 스마트폰용 앱 8418시전 및 영양 다운모드 사용으로 이용합니다. 문서 다운모드 ©
	KeyToken 구용 프로그램 KeyToken 구용 프로그램 KeyToken HSM 무정정 따라하기 KeyToken HSM Quick, Quide 2013/028.pdf KeyToken LHSM 에너희 KeyToken LHSM 에너희	1 성치파일 다운호도 © 문서 다운포도 @ 문서 다운포드 @
	KeyToken 구등 프로그램	स्रग्नाथ मध्यप्र 💿

그림 8. 실행파일 다운로드

※ microSD를 내장한 KeyToken MSD 제품 또는 KeyToken USB 제품은 미리 저장되어 있는 KeyTokenSetup.exe 파일을 사용하여 바로 [3] 단계를 진행하시면 됩니다. 2

3

그림 9 화면에서 '열기'를 선택합니다.

← → Ø http://www.keypair	戶 ~ 旨 C 🧐 Keypair 🛛 🗙	× n * ¤
f ?Keypair	• 회사소개 • 보안 하드웨어 • 보안 소프트웨어 • 다운로드	• 고객센티
 DOWNLOAD	Vindows Internet Explorer KeyTokenSetup.zip(으)로 무엇을 하시겠습니까? 크기: 13.1M8 위치: www.keypair.co.kr	
	● 열기(0) 파일이 자동으로 저장되지 않습니다 Ken USB ● 스마트환 ● 저장(S) 네 코르이름으로 저장(A) 분석 다운로	18 11 18 0.4 015 10-0
	복소 KeyToken HSM KeyToken 구동 프로그램 KeyToken 105.0.02 성치파일 다 KeyToken 105.0.01 KeyToken HSM 부력적 대원하기 KeyToken 105.0.046 _011201.001 문서 다운로 KeyToken 105.045 _011201.001 KeyToken Liber_Mana_20131001.001 문서 다운로	0 288 0 28 0 28
	KeyToken 전동 프로그램 설치미일 다	225 •

그림 9. KeyTokenSetup.zip 파일 열기



그림 10. KeyTokenSetup.exe 파일 실행하기

- ※ 그림 10에서, KeyTokenSetup.exe 파일은 운영체제의 환경설정에 따라 'KeyToken Setup'으로 표시될 수 있습니다.
- ※ KeyTokenSetup.exe 파일은 기능 향상을 위하여 수시로 변경될 수 있습니다. 이때, '클라우드 평판 기반 실행 차단' 기능을 가진 V3와 같은, 사용자 평가 기반의 백신 프로그램은 변경된 KeyTokenSetup.exe 파일 및 설치되는 실행 파일들을 새로운 프로그램으로 인식하여, 충분한 사용자 평가가 이루어지기 전까지 보안 경고를 표시할 수 있습니다.
- 또한, 운영체제 사용자 계정의 권한에 따라 그림 11과 같은 화면의 확인 메시지가 표시될 수 있습니다.
- ※ KeyTokenSetup.exe 파일 및 설치되는 실행 파일들에 대한 보안성은 당사에서 충분히 검증한 후 공개하므로, 안심하시고 실행을 허용하시면 됩니다.
- 3-1 그림 11과 같은 화면이 나타날 경우, '예' 버튼을 누릅니다.



그림 11. 실행 허용 선택하기

※ KeyTokenSetup.exe 파일을 실행하기 위해서는 윈도우 시스템에 'Microsoft .NET Framework 4.0 Client'가 설치되어 있어야 합니다. 윈도우 시스템이 Windows XP 이거나 Windows Vista 이상이라도 최신 업데이트가 적용되어 있지 않다면, 아래의 [3-2] ~ [3-4] 단계를 진행하시어 'Microsoft .NET Framework 4.0 Client'를 설치해야 합니다. 설치 시간은 PC 성능과 네트워크 사정에 따라서 수분에서 수십분이 소요 됩니다. 3-2 그림 12 화면에서 '설치' 버튼을 눌러, 'Microsoft .NET Framework 4.0 Client'의 설치를 시작합니다.



그림 12. Microsoft .NET Framework 4.0 Client 설치 시작

3-3 그림 13 화면에서 다운로드가 완료될 때까지 기다립니다. 네트워크 사정에 따라서 수분에서 수십분이 걸릴 수 있습니다.

상태	필수 요소
다운로드 중	Microsoft .NET Framework 4.0 Client
다운로드 중:	dotNetFx40_Client_x86_x64.exe
다운로드 중: • 남은 예상 시	dotNetFx40_Client_x86_x64.exe 간: 13 분 19 초

그림 13. Microsoft .NET Framework 4.0 Client 다운로드 중

3-4 그림 14 화면에서 설치가 완료될 때까지 기다립니다. PC 성능에 따라서 수분에서 수십분이 걸릴 수 있습니다.

[목미 설치되어 릭하십시오.	있어야 합니
121	할릭하십시오.

그림 14. Microsoft .NET Framework 4.0 Client 설치 중

E.	Ζ.	

그림 15 화면에서 '다음' 버튼을 눌러, KeyToken Manager의 설치를 시작합니다.



그림 15. KeyToken Manager 설치 시작

5 그림 16 화면이 나타나면 기다립니다.

설치 상태	124
InstallShield(R) 설치 마법사가 KeyToken Manager을(를) 설치하고 있습니다.	
stallShield	
	취소

그림 16. KeyToken Manager 설치 진행중

6 PC의 USB포트에 KeyToken이 연결되어 있지 않으면, 그림 17 화면이 나타납니다. PC의 USB포트에 KeyToken을 연결하십시오.

《 PC의 USB포트에 Key	Token를 연결하십시오.	취소
- KeyToken 초기화		
라벨(선택사항):		
사용할 비밀번호 :		
비밀변호 확인 :		
※ 라벨은 32자이히 ※ 비밀번호는 8자 합니다.	하의 문자 또는 숫자여야 합니다 이상 16자이하의 문자 또는 숫	다. 자여야
	초기화	

그림 17. KeyToken 찾기

7 PC의 USB포트에 연결된 KeyToken이 초기화되어 있지 않으면, 그림 18 화면이 나타납니다. KeyToken 비밀번호 등 초기화에 필요한 정보를 입력합니다.

🗶 KeyToken	을 찾았습니다. 초	기화하십시오.	취소	
— KeyToken	초기화			_
라벨(신	[택사항): 🖊		6	
사용할	비밀번호			
비밀번	호 확인 : 📐		/	
※ 라	별은 32자이하의 둔	자 또는 숫자여이	한다.	
※ 비역 합니	일변호는 8자이상 ' 니다.	16자이하의 문자 !	포는 숫자여야	
		초기화		

그림 18. KeyToken 초기화 정보 입력

8 그림 19 화면에서 '초기화' 버튼을 눌러, KeyToken을 초기화합니다.

KeyToken을 찾았습니	니다. 초기화하십시오. 취소
KeyToken 초기화 —	
라벨(선택사항):	이정엽 HSM
사용할 비밀번호 :	
비밀번호 확인 :	•••••
※ 라벨은 32자이 ※ 비밀번호는 87 합니다.	하의 문자 또는 숫자여야 합니다. 자이상 16자이하의 문자 또는 숫자여야
	초기화

그림 19. KeyToken 초기화 시작

9 그림 20 화면에서 '확인' 버튼을 눌러, KeyToken 초기화를 완료합니다.



그림 20. KeyToken 초기화 완료

10 그림 21 화면에서 '완료' 버튼을 눌러, KeyToken Manager의 설치를 완료합니다.



그림 21. KeyToken Manager 설치 완료

3. 구동 프로그램 삭제

이 절에서는 Windows 7에서 설치된 KeyToken 구동 프로그램을 삭제하는 과정을 예를 들어서 설명합니다. 기본적으로 Windows 8, Windows Vista, Windows XP에서도 동일한 과정으로 삭제합니다.

1 II장 2절의 '구동 프로그램 설치'에서 [1], [2], [3] 단계를 실행합니다.

※ 윈도우의 제어판에서 '프로그램 제거'를 선택한 후 'KeyToken Manager'를 찾아서 '제거'를 선택하셔도 됩니다.

2 그림 22 화면에서 '다음' 버튼을 눌러, KeyToken Manager의 삭제를 시작합니다.



그림 22. KeyToken Manager 삭제 시작

3 그림 23 화면이 나타나면 기다립니다.

설치 상태			N-24
InstallShield(R) 설치 마법사가 Key	yToken Manager을(를)) 제거하고 있습니다.	
stallShield			취소

그림 23. KeyToken Manager 삭제 진행중





그림 24. KeyToken Manager 삭제 완료

III. KeyToken Manager

KeyToken Manager는 공인인증서의 복사 및 삭제, 그리고 KeyToken의 초기화 및 비밀 번호 변경을 위한 KeyToken 관리 소프트웨어입니다.

1. 공인인증서 복사

KeyToken Manager는 공인인증서를 현재의 저장매체에서 다른 저장매체로 복사할 수 있습니다. 하지만 표 1과 같이, 공인인증서를 보안이 매우 취약한 하드 디스크로 복사 하는 것은 허용하지 않으며, 또한 한국인터넷진흥원(KISA)의 규격을 준수하여 보안토큰 안의 공인인증서를 다른 저장매체로 복사하는 것도 허용하지 않습니다.

공인인증서	하드 디스크로	이동식 디스크로	보안토큰으로	백업영역으로
위치	복사하기	복사하기	복사하기	복사하기
하드 디스크	불가능	가능	가능	가능
이동식 디스크	불가능	가능	가능	가능
보안토큰	불가능	불가능	불가능	불가능
백업영역	불가능	가능	가능	불가능

표 1. 공인인증서 복사 가능 저장매체

이 절에서는 하드 디스크에 저장되어 있는 공인인증서를 보안토큰과 백업영역으로 복사 하는 과정을 예를 들어서 설명합니다. 이동식 디스크 또는 백업영역에 저장되어 있는 공인인증서를 다른 저장매체로 복사하는 과정도 설명할 예와 기본적으로 동일합니다.

[1] 단계는 KeyToken Manager를 실행하는 과정이며, [2] ~ [6] 단계들은 하드 디스크의 공인인증서를 보안토큰으로 복사하는 과정이며, [7] ~ [11] 단계들은 하드 디스크의 공인 인증서를 백업영역으로 복사하는 과정입니다. 보안토큰에 저장된 공인인증서는 PC에서 사용할 수 있으며, 백업영역에 저장된 공인인증서는 PC와 NFC 스마트폰에서 사용할 수 있습니다. 먼저, PC의 USB 포트에 KeyToken을 연결한 후, 다음의 단계를 시작합니다.



윈도우의 바탕화면에서 그림 25와 같은 'KeyToken Manager' 아이콘을 찾아 더블 클릭하여, KeyToken Manager를 실행시킵니다.



그림 25. KeyToken Manager 아이콘

2 그림 26 화면에서 하드 디스크의 체크박스를 클릭하거나 공인인증서를 더블클릭 하여, 복사할 공인인증서를 선택합니다.

No. 상태 위치 소요자 용도 발급자 만큼일 이 유호 C:\Progr 이정엽(Ju 개인 금융 yessign 2013-06-14	보안철 보안물론 (최대 6개의 공인인증서를 저장할 수 있습니다.)
	110, 영대 소유사 영포 월급사 빈노일
I동식 디스크 No. 상태 위치 소유자 용도 발급자 만료일	- 저장된 공인인증서는 보안토큰 안에서만 사용되며, 외부로 복사할 수 없습니다. - 현재는 PC에서만 사용가능합니다. (NFC 스마트폰은 조만간 지원할 예정입니다.) 백업영역 (최대 1개의 공인인증서를 저장할 수 있습니다.)
- KeyToken MSD의 microSDLF KeyToken USB의 USB 메모리 안에 들어 있는 코인이즈 또는 이트시 디스크 아이 코인이즈 바르 프니티UTL	No. 상태 소유자 용도 발급자 만료일 - 개장된 공인인증서를 외부로 복원할 수 있습니다. - KeyToken App를 이용하여, NFC 스마트론해서도 공인인증서를 안전하게 사용하실 수 있습니다. (지세한 내용은 KeyToken App 때뉴얼을 참조하십시오.)
※ 선택된 공인인증사가 없습니다.	공연인증사 비밀번호 : 공연인증서 복사
에그먹스를 불덕하거나 동안안동서를 너물물덕하며, 먼저 동안안동서를 전덕하십시오. 이 보안토론 이 백업양역 이 미동식 디스크 -	KeyToken 비밀번호 : 공인인증서 삭제

그림 26. 복사할 공인인증서 선택

		-
	드	

3 그림 27 화면에서 공인인증서를 복사할 위치인 '보안토큰' 버튼을 선택합니다.

No. 상태 위치 소유자 용도 ! ▼1 유효 C:\\Progr 미경엽(Ju 개인 금융 y	발급자 만료일 essign 2013-06-04	- 보안칩 보인	·토콘 (최대 67	I의 공인인증서를 저질	양할 수 있습니[I.)	
		→ No	. 상태	소유자	용도	발급자	만료일
동식 디스크 No. 상태 위치 소유자 용도 !	발급자 만료일 <	- 저 - 현 백입	장된 공인인증 재는 PC에서민 영역 (최대 17	서는 보안토큰 안에서 ! 사용가능합니다. (Ni i의 공인인증서를 저장	만 사용되며, 1 FC 스마트폰은 양할 수 있습니[비부로 복사할 조만간 지원할 다.)	수 없습니다. 알 예정입니다.)
- KeyToken MSD의 microSDL+ KeyToken USB의 USB 메	모리 안에 들어 있는	> No - 7त - Ka - Ka	, 상태 장된 공인인증 ayToken Appi 용하실 수 있습	소유자 서를 외부로 복원할 수 을 이용하며, NFC 스미 니다. (자세한 내용은	용도 2 있습니다. IF트폰에서도 공 KeyToken Ap	발급자 인인증서를 인 p 매뉴얼을 침	만료일 !전하게 조하십시오.)
공인인증서는 이동식 디스크 안의 공인인증서로 표시됩니! * 선택한 하드 디스크의 공인인증서는 복사하거나 식?	다		198 8 - 1			[

그림 27. 복사할 위치 선택

4 그림 28 화면에서 공인인증서 비밀번호와 KeyToken 비밀번호를 입력합니다.

lo. 상태 위치 소유자 용도 발급자 만료일 l 유효 C:WProgr 이공업(Ju 개인 금융 yessign 2013-06-04 보안토르 (최대 6개의 공인인증서를 제장할 수 있습니다.) No. 상태 소유자 용도 발급자 만료일 4 디스크 - 저장된 공인인증서는 보안토르 안에서만 사용되며, 외부로 특사할 수 있습니다.) No. 상태 위치 소유자 용도 발급자 만료일 - 저장된 공인인증서는 보안토르 안에서만 사용되며, 외부로 특사할 수 있습니다.) No. 상태 위치 소유자 용도 발급자 만료일 No. 상태 위치 소유자 용도 발급자 만료일 No. 상태 유지자 용도 발급자 만료일 No. 상태 소유자 용도 발급자 만료일 · 저장된 공인인증서를 제약할 수 있습니다. · KeyToken MSD의 microSDL KeyToken USB의 USB 때문리 안에 들어 있는 공인인증서 비밀번호와 KeyToken 비밀번호를 일억하십시오.			=						KeyToken —					
전 1 유효 C:₩Progr 미장입(Ju 개인 금융 yessign 2013-06-04 보안토관 (최대 6개의 공인인증서를 재장할 수 있습니다.) No. 상태 소유자 용도 발급자 만료일 4 디스크 - 저장된 공인인증서는 보안토관 안에서만 사용되며, 외부로 특사할 수 있습니다.) - 저장된 공인인증서는 보안토관 안에서만 사용되며, 외부로 특사할 수 있습니다.) - 전쟁는 PC에서만 사용가능입니다. (NFC 스마트폰은 조만간 지정할 예정입니다.) 백업영역 (최대 1개의 공인인증서를 재장할 수 있습니다.) No. 상태 소유자 용도 발급자 만료일 - 저장된 공인인증서를 제장할 수 있습니다.) No. 상태 소유자 용도 발급자 만료일 - 저장된 공인인증서를 제장할 수 있습니다.) No. 상태 소유자 용도 발급자 만료일 - 저장된 공인인증서를 제장할 수 있습니다.) No. 상태 소유자 용도 발급자 만료일 - 저장된 공인인증서를 제당할 수 있습니다.) - 전환한 하도 디스크의 양의 양인증서를 보안토픈으로 복사할 수 있습니다. 공인인증서 비밀번호와 KeyToken 비밀번호를 입력하십시오.	P	lo,	상태	위치	소유자	용도	발급자	만료일	보안칩 -					
식 디스크 - 재장된 공인인증서는 보안토르 안에서만 사용되며, 외부로 특사할 수 없습니다. 44 디스크 - 재장된 공인인증서는 보안토르 안에서만 사용되며, 외부로 특사할 수 없습니다. 46. 상태 위치 소유자 용도 발금자 만료일 - · · · · · · · · · · · · · · · · · · ·		1	유효	C:₩Progr	이정엽(Ju	개인 금융	yessign	2013-06-04	보안토	큰 (최대 67	H의 공인인증서를 저장	'할 수 있습니C	ł.)	
식 디스크 - 저장된 공연인증서는 보안토르 안에 새한 사용되며, 외부로 복사할 수 없습니다. - 현재는 PC에 새한 사용가능합니다. (NFC 스마트폰은 조만간 지원할 예정입니다.) 백업양역 (최대 1계의 공연인증서를 제장할 수 있습니다.) No. 상태 소유자 용도 발급자 만료일 - 저장된 공연인증서를 제장할 수 있습니다.) No. 상태 소유자 용도 발급자 만료일 - 저장된 공연인증서를 제장할 수 있습니다.) - 저장된 공연인증서를 제상할 수 있습니다. - Key Token App를 미용하며, NFC 스마트폰에서도 공연인증서를 안전하게 사용하실 수 있습니다. (지세한 내용은 Key Token App 매뉴일을 참조하십시오.) * 선택한 하도 디스크의 공연인증서를 보안토큰으로 복사할 수 있습니다. 공연인증서 비밀번호와 Key Token 비밀번호를 입력하십시오.									No,	상태	소유자	용도	발급자	만료일
KeyToken MSD의 microSDL: KeyToken USB의 USB 배모리 안해 들어 있는 · 제장된 공인인증서를 외부로 복원할 수 있습니다. · KeyToken App를 이용하여, NFC 스마트론에서도 공인인증서를 안전하게 · KeyToken App를 이용하여, NFC 스마트론에서도 공인인증서 비용을 참조하십시오.) · KeyToken App를 이용하여, NFC 스마트론에서도 공인인증서 비용을 참조하십시오.) · KeyToken App를 이용하여, NFC 스마트론에서도 공인인증서 비용을 참조하십시오.) · KeyToken Hag번호를 입력하십시오. · · · · · · · · · · · · · · · · · · ·	15	닉 디 Jo.	스크 -	위치	소유자	용도	발급자	만료일	- 저장 - 현재 백업영 No,	인 공인인증 = PC에서민 역 (최대 17 상태	서는 보안토큰 안에서 안 사용가능합니다. (NF 태의 공인인증서를 저장 소유자	만 사용되며, 오 FC 스마트폰은 함말 수 있습니다 용도	부로 복사할 조만간 지원할) 발급자	수 없습니다. 날 예정입니다.) 만료일
* 선택한 하드 디스크의 공인인증서를 보안토큰으로 복사할 수 있습니다. 공인인증서 비밀번호와 KeyToken 비밀번호를 입력하십시오.	the second	Key T	oken I중서	MSD의 microS = 이동식 디스	DLF KeyToker 키 아의 공인이용) USB의 USE 즉서로 표시된	3 메모리 안이	에 들어 있는	- 저장! - KeyT 사용8	인 공인인증 oken Appi 바실 수 있습	서를 외부로 복원할 수 을 이용하여, NFC 스마 니다. (자세한 내용은	있습니다. 트폰에서도 공 KeyToken Apj	인인증서를 인 p 매뉴얼을 참	'전하게 조하십시오.)
		종인연 ※	신택한 공연	는 이동식 디스크 하드 디스크의 인인증서 비밀번	코 안의 공인인종 공인인증서를 I호와 KeyToke	중서로 표시됨 보안토큰으릐 n 비밀번호를	입니다. 로 복사할 수 중 입력하십시	있습니다. I오,	공인인증서 비밀번	호 :			æ	인인증서 복사

그림 28. 비밀번호 입력

								но	ын					
N		상태	위치	소유자	용도	발급자	만료일	F + -		-				
V	E S	유표	C:WProgr	이성엽(Ju,,,	개인 금융	yessign	2013-06-04		퀸안토 Ma	큰 (최대 6기	H의 공인민증서를 저질	양할 수 있습니[으로	.ł.)	DL =01
									NO,	StH	조유사	용도	말급사	만료일
_	_													
_ ,	-	-							지장	되 고이이주	서는 보아트크 아메셔!	or traciut a	연내보 드브	스 연습니다
5.	11	:= -						-	현재	는 PC에서면	반 사용가능합니다. (NF	FC 스마트폰은	조만간 지원	할 예정입니다.)
N	i. 1	상태	위치	소유자	용도	발급자	만료일		-	04 (÷IFU 17	이 고이이즈 나르 고즈	bet 스 이스니 I	1)	
									No.	상태	소유자 소유자	8도 ····································	-r./ 발급자	만금일
									저장	된 공인인증	서를 외부로 복원할 수	: 있습니다.		
								-	Key	Foken Appi	을 이용하며, NFC 스미 네트니 (TLM하니 용으	사트폰에서도 공	인인증서를 인	반전하게 H조국LALUON
- 1	ByTo	ken I	MSD의 micros	SDLI KeyToker	USB의 USE	8 메모리 안(베 들어 있는		VIE		니다. (세제한 대중은	Key lokeli Mp	puinee e	(±018/1±.)
Ch1	인인	증서는	E 이동식 디스.	크 안의 공인인?	동서로 표시될	ULICH,								
												5		
	×	백한	하드 디스크의	I 공인인증서를	보안토큰으로	로 복사할 수	있습니다.	2이이증서	비밀브	1÷ : .				2이이증서 봉사
	200	-	·민증서 비밀변	변호와 KeyToke	n 비밀변호를	를 입력하십시	1오.						-	22014 114
		36												

5 그림 29 화면에서 '공인인증서 복사' 버튼을 누릅니다.

그림 29. 공인인증서 복사

6 그림 30 화면에서 '확인' 버튼을 눌러, 하드 디스크의 공인인증서를 보안토큰으로 복사하는 과정을 완료합니다.

No,	상태 유효	위치 C:\Progr	소유자 이정엽(Ju,	용도 개인 금융	발급자 yessign	만료일 2013-06-04	보안칩 - 보안됩	큰 (최[내 6개의 공민인증서를 저장할	수 있습니다	.)	0.20
							No.	유효	소유사 이정엽(Jung Youp Lee)	용도 개인 금융	말급사 yessign	만료일 2013-06-04
이동식 C No.	니스크 상태	위치	소유자	85	발급자	CeyToken Manager			보안토큰 안에서만 기능합니다. (NFC	사용되며, 외 스마트폰은 : 수 있습니다	부로 복사할 조만간 지원]	수 없습니다. 활 예정입니다.)
- Key	Token	MSD의 microS	DLF KeyToker		3 메모리 언	· 문어 있는		종니니 확(소유자 외부로 복원할 수 있 하여, NFC 스마트 (자세한 내용은 Ke 	용도 !습니다. 폰에서도 공연 yToken App	발급자 인인증서를 연 매뉴얼을 침	만료일 안전하게 당조하십시오.)
공인	문 클리	는 미봉식 니스: ※ 선	크 안의 공인인(1백된 공인인증 주서를 더블클릭	응서로 표시템 서가 없습니[말하여 며게	니다. 다. 고이이즈 서	르 셔택치시시오	공인인증서 비밀법	1호 : [2	용인인증서 복사
	글 클릭	하거나 공인인	증서를 더불클릭	릭하며, 먼저	공인민증서	를 선택하십시오.	8008A 08	: - · ·]			-	5008A 9A

그림 30. 공인인증서 복사 완료

f[®]Keypair

7 그림 31 화면에서 하드 디스크의 체크박스를 클릭하거나 공인인증서를 더블클릭 하여, 복사할 공인인증서를 선택합니다.

Token Manager v2000 인증서 관리 [KeyToken 관리 www.keypair.co.kr] - 하드 디스크	KeyToken
7 No. 상태 위치 소유자 용도 발급자 만료일	도 보안칩
·····································	보안토린 (3대 6채의 왕인인동사를 제장할 수 있습니다.) No, 상태 소유자 용도 발급자 만료입 ☐ 1 유효 이정엽(Jung Youp Lee), 개인 금융 yessign 2013-06-04
- 이동석 디스크 No. 상태 위치 소유자 용도 발급자 만료일	- 저장된 공연인증서는 보안토큰 안에서만 사용되며, 외부로 복사할 수 없습니다. - 현재는 PC에서만 사용가능합니다. (NFC 스마트폰은 조만간 지원할 예정입니다.) 백업영역 (최대 1개의 공인인증서를 저장할 수 있습니다.) No. 상태 소유자 용도 발급자 만료일
- KeyToken MSD의 microSD나 KeyToken USB의 USB 메모리 안해 들어 있는 공인안증서는 이동식 디스크 안의 공인인증서로 표시됩니다.	- 저장된 공인인증서를 외부로 복원할 수 있습니다. - KeyToken App를 이용하며, NFC 스마트폰에서도 공인인증서를 안전하게 사용하실 수 있습니다. (자세한 내용은 KeyToken App 매뉴얼을 참조하십시오.)
× 선택된 공인인증서가 없습니다. 쳐크박스를 클릭하거나 공인인증서를 대불클릭하여, 먼저 공인인증서를 선택하십시오. 이 보안토리 이 백업명역 이 마동식 디스크 💌	공인인증서 배월번호 : 프린인증서 북사 KeyToken 비밀번호 : 프린인증서 삭제
※ USB 포트에 KeyToken HSMOI 연결되어 있습니다.	프로그램 종료

그림 31. 복사할 공인인증서 선택

8 그림 32 화면에서 공인인증서를 복사할 위치인 '백업영역' 버튼을 선택합니다.

No. 상태 위치	소유자	용도 발급	3자 만료일		- 보안칩 - 티아트	= /≯I	비에기에주니르 기자하		```	
						은 (최대 상태 유효	소유자 이정엽(Jung Youp Lee)	용도 개인 금융	./ 발급자 yessign	만료일 2013-06-04
동식 디스크 No. 상태 위치	자유소	용도 발급	금자 만료일 •		- 저장 - 현재 백업영	된 공인 는 PC0 역 (최[인증서는 보안토큰 안에서만 서만 사용가능합니다. (NFC # 1개의 공인인증서를 저장할	사용되며, 외 스마트폰은 수 있습니다	부로 복사할 조만간 지원' .)	수 없습니다. 할 예정입니다.)
- KeyToken MSD의 m 공인인증서는 미동식	croSDLł KeyToken U 디스크 안의 공인인증서	SB의 USB 메모i 네로 표시됩니다.	리 안에 들어 있는		→ No, - 저장 - Key 사용i	상태 된 공인 Token i 하실 수	소유자 인증서를 외부로 복원할 수 있 App을 이용하며, NFC 스마트 있습니다. (자세한 내용은 Ke	용도 [습니다. 폰에서도 공연 yyToken App	발급자 인인증서를 9 메뉴얼을 참	만료일 안전하게 상조하십시오.)
※ 선택한 하드 디	스크의 공인인증서는 복	사하거나 삭제할	알 수 있습니다. o	공인인	!증서 비밀빈	1호: [동안인증서 복사

그림 32. 복사할 위치 선택

	-1-	3						L K	KeyToken —					
6	ö,	상태	위치	소유자	용도	발급자	만료일	_	▶ 보안칩					
1	1	유효	C:₩Progr	이정엽(Ju	개인 금융	yessign	2013-06-04		보안	토큰 (최	대 6개의 공인인증서를 저장할	수 있습니다	.)	
									No,	상태	소유자	용도	발급자	만료일
										유효	이정엽(Jung Youp Lee)	개인 금융	yessign	2013-06-04
1	_													
동		스크							- 733	장된 공인	인증서는 보안토큰 안에서만	사용되며, 외	부로 복사할	수 없습니다.
6	•	AFEU	외귀	AON	80	바그지	마군의		- 연/	#≘ PCI	베서만 사용가등합니다. (NFC	스마트폰은	소만간 시원	할 예정입니다.)
P	0.	041	7174	1414	01	20/1	CHE		백업	명역 (최	대 1개의 공인인증서를 저장할	수 있습니다	.)	
F									> No,	상태	소뮤자	용도	발급자	만료일
									- 787	- 모 고 0	이즈 사로 이보고 보의한 스 이			
									- Ke	Token	App을 이용하여, NFC 스마트	폰에서도 공연	인인증서를 연	안전하게
-	ev]	oken	MSD21 micro	SDL F Key Toker	USB2I USP	3 M 9 21 9 4	세 들어 있는		사용	하실 수	있습니다. (자세한 내용은 Ke	yToken App	매뉴얼을 칠	남조하십시오.)
	121	· 중시	는 이동식 디스	크 안의 공인인	동서로 표시될									
	×	서태하	하드 디스크의	이 공이이주서를	배 <u>어</u> 영영으a	금 봉사학 스								
			KevT	oken 비밀변호	응 입력하십시	19		공인	l인증서 비밀	번호 :			Ę	공인인증서 복사
							[F .]	9				-		
			C 3	0 <u><u><u></u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u>	021 114			K KAU	I OKEN LIS	19:1				날아이 중 세 실제

9 그림 33 화면에서 KeyToken 비밀번호를 입력합니다.

그림 33. 비밀번호 입력

10 그림 34 화면에서 '공인인증서 복사' 버튼을 누릅니다.

	리스:	3							KeyToken —					
N	0,	상태	위치	소유자	용도	발급자	만료일		▶ 보안칩					
V	1	유효	C:₩Progr	이정엽(Ju	개인 금융	yessign	2013-06-04		보안트	[큰 (최	대 6개의 공인인증서를 저장할	수 있습니다	.)	
									No,	상태	소유자	용도	발급자	만료일
									1	유효	미정엽(Jung Youp Lee)	개인 금융	yessign	2013-06-04
N	╡ []: o,	스크 - 상태	위치	소유자	용도	발급자	만료일		- 저경 - 현지 백업영 No,	1년 공인 1는 PCC 명역 (최미 상태	인증서는 보안토큰 안에서만 에서만 사용가능합니다. (NFC 대 1개의 공인인증서를 저장할 소유자	사용되며, 외 스마트폰은 수 있습니다 용도	부로 복사할 조만간 지원] .) 발급자	수 없습니다. 할 예정입니다.) 만료일
- 10	leyTi 중인인	oken 1 !중서는	MSD의 microS 5 이동식 디스크	DLH KeyToker 코 안의 공인인용	USB의 USE 동서로 표시됩	에 모리 안() [니다.	네 들어 있는		- 제주 - Key 사용	'된 공인 Token 하실 수	[민증서를 외부로 복원할 수 있 App을 미용하여, NFC 스마트, 있습니다. (자세한 내용은 Ke	(습니다. 폰에서도 공연 syToken App	인인증서를 연) 매뉴얼을 침	안전하게 남조하십시오.)
	* :	선택한	하드 디스크의 KeyTo	공인인증서를 oken 비밀변호를	백업영역으로 등 입력하십시	문 복사할 수 I오,	있습니다.	30	인인증서 비밀	친호 :		10		응인인증서 복사

그림 34. 공인인증서 복사

1°Keypair

11 그림 35 화면에서 '확인' 버튼을 눌러, 하드 디스크의 공인인증서를 백업영역으로 복사하는 과정을 완료합니다.

No.	:크 상태 유효	위치 C:₩Progr	소유자 이정엽(Ju,	용도 개인 금융	발급자 yessign	만료일 2013-06-04	- Keyloken	큰 (최[대 6개의 공인인증서를 저장할	수 있습니다	.)	
							No.	상태 유효	소유자 미정엽(Jung Youp Lee)	용도 개인 금용	발급자 yessign	만료일 2013-06-04
이동식 C	스크 -				C	KeyToken Manager			보안토큰 안에서만 가능합니다. (NFC	사용되며, 외 스마트폰은 :	부로 복사할 조만간 지원]	수 없습니다. 할 예정입니다.)
No.	상태	위치	소유자	용도	발급자	ਹਿ ਤੁਹੁਹੂਤੂ	서를 성공적으로 복사하였	(습니디 확인	다. 소유자 ung Youp Lee) 외부로 복원할 수 있 하며, NFC 스마트 (Trul of these Ke	수 있습니다 용도 개인 금융 습니다. 폰에서도 공연	.) 발급자 yessign 인인증서를 인	만료일 2013-06-04 안전하게 상조하십시오)
- Key 공인	Token I 인증서는	MSD의 microS 는 이동식 디스:	SDL+ KeyToker 크 안의 공인인	NUSB의 USE 중서로 표시될	3 메모리 안 1니다.	케 들어 있는		_		yrononnipp		12018/02/7
체크박스	등 금덕	※ 선 하거나 공인인	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	서가 없습니! 릭하여, 먼저	다. 공인인증서:	를 선택하십시오.	공인인증서 비밀번	호 : [Ē	공인인증서 복사
) 보안!	E2	🔿 백업영역	0 015	통식 티스크	*	KeyToken 비밀번	± ∶ Γ			3	중인인증서 삭제

그림 35. 공인인증서 복사 완료

* 백업영역에 저장된 공인인증서는 그림 36과 같이 KeyToken App을 이용하여 NFC 스마트폰으로 복사할 수 있습니다. 자세한 내용은 'KeyToken App Manual'을 참조 하시기 바랍니다.



그림 36. KeyToken App 설치 QR 코드 및 실행 화면

2. 공인인증서 삭제

KeyToken Manager는 하드 디스크, 이동식 디스크, 보안토큰, 백업영역에 저장되어 있는 공인인증서를 삭제할 수 있습니다.

이 절에서는 하드 디스크에 저장되어 있는 공인인증서를 삭제하는 과정을 예를 들어서 설명합니다. 이동식 디스크, 보안토큰, 백업영역에 저장되어 있는 공인인증서를 삭제하는 과정도 설명할 예와 기본적으로 동일합니다.

먼저, PC의 USB 포트에 KeyToken을 연결한 후, 다음의 단계를 시작합니다.

- 1 III장 1절의 '공인인증서 복사'에서 [1] 단계를 실행하여, KeyToken Manager를 실행 시킵니다.
- 2 그림 37 화면에서 하드 디스크의 체크박스를 클릭하거나 공인인증서를 더블클릭 하여, 삭제할 공인인증서를 선택합니다.

KeyToken Manager v2000 공인연증서 관리 KeyToken 관리 www.keypair.co.kr	
하드 디스크 2 No, 상태 위치 소유자 용도 발급자 만료일 - 1 유효 C:\\Progr 이정엽(Ju 개인 금융 yessign 2013-06-02	KeyToken
	No. 상태 소유자 용도 발급자 만료일 ■ 1 유효 이정엽(Jung Youp Lee) 개인 금융 yessign 2013-06-04
이동식 디스크 No. 상태 위치 소유자 용도 발급자 만료일	- 저장된 공인인증서는 보안토큰 안에서만 사용되며, 외부로 복사할 수 없습니다. - 현재는 PC에서만 사용가능입니다. (NFC 스마트폰은 조만간 지원할 예정입니다.) 백업업역 (최대 1개의 공인인증서를 저장할 수 있습니다.)
- KeyToken MSD의 microSDLF KeyToken USB의 USB 해도리 안에 들어 있는	No. 상태 소유자 용도 말급사 만료일 1 유호 (1) 정갑(Jung You Lee) 개인 금용 yessign 2013-06-04 - 저장된 공인인동사를 외부로 특별할 수 있습니다. - Key Token App를 이용하며, NFC 스마트폰에서도 공인인동사를 안전하게 사용하실 수 있습니다. (자세한 내용은 Key Token App 매뉴얼을 참조하십시오.)
공인인증서는 이동식 디스크 안의 공인인증서로 표시됩니다. ※ 선택된 공인인증서가 없습니다. 체크박스를 클릭하거나 공인인증서를 더불클릭하며, 먼저 공인인증서를 선택하십시오.	공인인증서 비밀번호 : 공인인증서 복사
○ 보안토큰 이 백입영역 ○ 이동식 디스크 ▼ × USB 포트에 KeyToken HSMOI 연결되어 있습니다.	KeyToken 비밀번호 : 공인인정시 삭제 프로그램 종료

그림 37. 삭제할 공인인증서 선택

ΞC	스크 —							KeyToke	n —					
No	상태	위치	소유자	용도	발급자	만료일	51	L 독등	'칩 -					
V	유효	C:\Progr	- 미정엽(Ju	개인 금융	yessign	2013-06-04		1	코안토	큰 (최[대 6개의 공인인증서를 저장할	수 있습니다	.)	
								->	No,	상태	소유자	용도	발급자	만료일
									1	유효	이정엽(Jung Youp Lee)	개인 금융	yessign	2013-06-04
No	상태	위치	소유자	용도	발급자	만료일 <			현재 백업영 No,	는 PC0 역 (최대 상태 유효	에서만 사용가능합니다. (NFC 대 1개의 공인인증서를 저장할 소유자 미정엽(Jung Youp Lee)	스마트폰은 수 있습니다 용도 개인 금융	조만간 지원 .) 발급자 yessign	할 예정입니다. 만료일 2013-06-04
- Ke 공!	yToken № 인인증서는	ISD의 micro 이동식 디스	SDLF KeyToker 크 안의 공인인(iUSB의 USI 중서로 표시됩	3 메모리 안에 합니다.	돌며 있는			·저장 Key 사용	된 공인 Foken i 하실 수	인증서를 외부로 복원할 수 있 App을 이용하며, NFC 스마트 있습니다. (자세한 내용은 Ke	!습니다. 폰에서도 공연 ryToken App	인인증서를 인 매뉴얼을 참	반전하게 남조하십시오.)
	※ 선택한	하드 디스크 복사하려면	의 공인인증서는 아래의 복사할	: 복사하거니 위치를 선택	· 삭제할 수 있 하십시오,	성습니다.	공연	인민증서	비밀빈	!호 : [3		응인민증서 복시
	-	-	HHOHOROR	OI	도신 티스크	E· _	Ka	uTokon k	ланы	÷				

그림 38. 공인인증서 삭제

Δ	

그림 39 화면에서 '예' 버튼을 눌러, 삭제함을 확인합니다.

3 그림 38 화면에서 '공인인증서 삭제' 버튼을 누릅니다.

드	스크 —						- KeyTo	ken —					
No	. 상태 1 8호	위치 C WProor	소유자	용도 게이 구유	발급자	만료일 2012-06-04	יז (ה	년안칩 ·	/ -			,	
	1 172	C.WFI0gI	018 8 (00	/12 68	yessigii	2013-00-04		> No, ■ 1	2큰 (최) 상태 유효	내 에너디 동안인동시들 세상을 소유자 미정엽(Jung Youp Lee)	유 있습니다 용도 개인 금융	.) 발급자 yessign	만료일 2013-06-04
No	디스크 . 상태	위치	소유자	용도	KeyToka	en Manager 선택한 하드 디스	2코의 공인인증/ 4	여를 삭⊼ 예(Y)	ৰাকনাই স	문 안에서만 나니다. (NFC 5.서를 저장할 자 이나요(N) 지역 100 Lee) 북원할 수 있 NFC 스마트	사용되며, 외 스마트폰은 : 수 있습니다 용도 개인 금융 (습니다. 폰에서도 공연	부로 복사할 조만간 지원] .) 발급자 yessign	수 없습니다. 탈 예정입니다.) 만료일 2013-06-04
- Ke 공	eyToken 민인증서	MSD의 microS 는 이동식 디스:	SDLF KeyToker 크 안의 공인인(n USB의 USE 증서로 표시됩	3 에 <u>보리 안</u> 0 1니다.	1 들어 있는			_	20 대용은 Ke	ey token App	배규걸걸 얻	'조아쉽지도,)
	※ 선택	한 하드 디스크의 복사하려면	의 공인인증서는 아래의 복사할	- 복사하거나 위치를 선택:	삭제할 수 ? 하십시오,	있습니다.	공인인증	서 비밀	번호 :			3	응인인증서 복사
		ĘB	◎ 백업영역	O 018	동식 디스크	E: 🗸	KevToke	n 비밀빈	1호:	<u> </u>		-	<u> -</u>

그림 39. 공인인증서 삭제 확인

-	디스	∃ —						_ Key	yToker	-					
	No.	상태	위치	소유자	용도	발급자	만료일	al r	- 보안	칩 —					
1	<u>v</u> 1	11.	C.WProgr	0188400	12 88	yessign	2013*00*04			인토 (No.] 1	은 (최대 6개 상태 유효 미정	의 공인인용서들 서양일 소유자 d엽(Jung Youp Lee)	주 있습니다 용도 개인 금융	.) 발급자 yessign	만료일 2013-06-04
5	식 디 No.	스크 상태	위치	소유자	용도	발급지	KeyToken Manager					오만토큰 안에서만 가능합니다. (NFC	사용되며, 외 스마트폰은 :	부로 복사할 조만간 지원	· 수 없습니다. 할 예정입니다.)
							A 정말로 삭	제하시겠습니	I771-2		, m ol ol i	인원용서를 세상을 소유자 ung Youp Lee) 1부로 복원할 수 9	위수 있습니다 용도 개인 금융 있습니다.	.) 발급자 yessign	만료일 2013-06-04
-	Key 공인9	Token 인증서	MSD의 microS 는 이동식 디스:	DLI KeyToker 크 안의 공인인용	IUSB의 USE 동서로 표시될	비모리 달	VI 201.244		m		아니요(N)	하여, NFC 스마트 자세한 내용은 Ka	폰에서도 공연 eyToken App	인인증서를 () 매뉴얼을 침	안전하게 함조하십시오.)
	*	(선택	한 하드 디스크의 복사하려면	의 공인인증서는 아래의 복사할	: 복사하거나 위치를 선택:	삭제할 수 하십시오,	있습니다.	공인인	!중서 E	미밀번	¢ : [[i	공인인증서 복사
	0	보안	토큰	🔿 백업영역	015	등식 디스크	E: 🔻	KeyTo	oken H	말번:	Σ:				공인인증서 삭제

5 그림 40 화면에서 '예' 버튼을 눌러, 삭제함을 다시 확인합니다.

그림 40. 공인인증서 삭제 재확인

그림 41 화면에서 '확인' 버튼을 눌러, 하드 디스크의 공인인증서를 삭제하는 과정을
 완료합니다.

No.	상태	위치	소유자	용도	발급자	만료일	F KeyToken - 보안칩 보아	 토크 (치	대 6개의 곳이이주서를 저장학	수 있습니다	.)	
							No	상태 이 유효	소유자 소유자 미정엽(Jung Youp Lee)	용도 개인 금융	방급자 yessign	만료일 2013-06-04
미동식 [No. - Key 공인	니스크 상태 VToken MSD	위치 의 microSDI 등식 디스크	소유자 나 KeyToken 안의 공인인공	용도 USB의 USE 서로 표시된	발급자 8	eyToken Manager 한 공인인증서 들어 있는	를 성공적으로 삭제 6 	₩였습니। 확	로 안도 한 번째 사망 가능합니다. (NFC 인인 중사를 저장할 소유자 ung Youp Lee) 리부로 복원할 수 있 (T/세한 내용은 Ke	사용되며, 외 스마트폰은 : 용도 개인 금융 입니다. 폰에서도 공연 yToken App	부도 독사할 조만간 지원] .) 발급자 yessign 인인증서를 인 이매뉴얼을 침	수 없습니다. 한료일 2013-06-04 산전하게 상조하십시오.)
	※ 선택한 하 8	E 디스크의 사하려면 아	공인인증서는 레의 복사할	복사하거니 위치를 선택	· 삭제할 수 있 하십시오,	làun.	공인인증서 비밀	번호 :			2	응인민증서 복사

그림 41. 공인인증서 삭제 완료

3. KeyToken 초기화

KeyToken은 정상사용상태이든 잠김상태이든 언제든지 초기화할 수 있습니다. 초기화시 KeyToken 비밀번호와 보안토큰, 백업영역 안의 모든 데이터는 완전히 삭제되므로, KeyToken 비밀번호를 새로 설정해야 하고 공인인증서도 새로 발급받거나 다시 복사해 넣어야 합니다. 하지만, KeyToken MSD의 microSD나 KeyToken USB의 USB 메모리 안의 데이터는 삭제되지 않습니다.

이 절에서는 KeyToken Manager로 KeyToken을 초기화하는 과정을 예를 들어서 설명 합니다.

먼저, PC의 USB 포트에 KeyToken을 연결한 후, 다음의 단계를 시작합니다.

- 1 III장 1절의 '공인인증서 복사'에서 [1] 단계를 실행하여, KeyToken Manager를 실행 시킵니다.
- 2 그림 42 화면에서 'KeyToken 관리' 탭을 선택합니다.

	상태	위치	소유자	용도	발급자	만료일	모 보안칩					
							보안태	E큰 (최	대 6개의 공인인증서를 저장할	수 있습니다	.)	
							No,	상태	소유자	용도	발급자	만료일
							1	유효	이정엽(Jung Youp Lee)	개인 금융	yessign	2013-06-04
	Token MS	D의 microS	DLF KeyToker	USB의 US	B 메모리 안에 티 미드	I 들어 있는	[] 1 - 저경 - Key 사용	유효 당된 공연 Token 하실 수	미정엽(Jung Youp Lee) !민증서를 외부로 복원할 수 있 App을 이용하며, NFC 스마트 ! 있습니다. (자세한 내용은 Ke	개인 금융 (습니다. 폰에서도 공연 ryToken App	yessign 인인증서를 연 매뉴얼을 침	2013-06-04 반전하게 남조하십시오.)
- Key	이 주서는 (1011111										
- Key 공인 크박스	인증서는 (※ 선 거나 공인인	택된 공인인증 증서를 더블클릭	서가 없습니 N하며, 먼저	다. 공인인증서를	# 선택하십시오.	공인인증서 비밀	번호 :				응인인증서 복사

그림 42. KeyToken 관리 탭 선택

3	그림 43 화면(에서 KeyToken	비밀번호 등	초기화에	필요한	정보를	입력합니다.
---	-----------	-------------	--------	------	-----	-----	--------

보안토큰미란?	- KeyToken 제품 정보	
물리적 보안 및 암호 연산 기능을 가진 첩을 내장하고 있어 해킹 등으로부터 공인인증서 유출을 방지하는 기능을 가진 안견성이 강화된 휴대용 공인인증서 저장매체입니다. - 한국인터넷진홍원(KISA) 홈페이지 중에서 -	제조사: Keypair 모델명: KeyToken HSM H/Wiver,: [1,0	
KeyToken은	F/W ver. : 1.0	
NFC를 지원하는 스마트폰에서도 공인인증서를 안전하게 사용할 수 있는 보안토르입니다. KeyToken HSM/MSD/USB 등의 모델이 있습니다.	S/N: 0001101000000001 사용상태: 정상적으로 동작중입니다.	도망의 KeyToken HSM의 구성도
- KeuToken 앱 섬치 : 08코드 (아드로미드용)	- KeuTaken *7181	
	3 計測(内部人体): DP2 HSM	혀재의 비밀번호 :
ente	사용할 비밀번호	변경할 비밀번호 :
	비밀번호 확인 :	비밀번호 확인 :
79至25226	※ KeyToken 보안칩 (보안토콘 + 백업영역) 안의	※ 비밀번호는 8자이상 16자이하의 문자 또는 숫자여야
	모든 데이터가 조가와됩니다. ※ KeyToken MSD의 microSDLF KeyToken USB의	입니다. ※ 현재의 비밀번호가 5회이상 연속으로 틀리면
	USB 메모리 한의 데이터는 적제되지 않습니다.	Keyloken의 모안집은 사용으로 점갑니다.
	초기화	비밀번호 변경

그림 43. KeyToken 초기화 정보 입력

4	그림 44	화면에서	'초기화'	버튼을	누릅니다.	

보안토르이란? 물리적 보안 및 암호 연산 기능을 가진 칩을 내장하고 있어 해킹 등으로부터 공인인증서 유출을 방지하는 기능을 가진 안견성이 강화된 휴대용 공인인증서 저장매체입니다. - 한국인터넷진홍원(KISA) 홈페이지 중에서 -	KeyToken 제품 정보 제조사 : Keypair 모델명 : KeyToken HSM H/W ver, : [1,0	
KeyToken은 NFC를 지원하는 스마트폰에서도 공인인용서를 안전하게 사용할 수 있는 보안토클입니다. KeyToken HSM/MSD/USB 등의 모델이 있습니다.	F/W ver. : [1.0 S/N : 0001101000000001 사용상태 : [정상적으로 동작중입니다.	KeyToken HSM의 구성도
- KeyToken 앱 설치 : OR코드 (안드로이트용)	KeyToken 초기화 라별(선택사학): 미징엽 HSM 사용할 비밀번호: ••••••••••••••••••••••••••••••••••••	Key Token 비밀번호 변경 현재의 비밀번호 : 변경할 비밀번호 : 비밀번호 확인 : ※ 비밀번호는 8자이상 16자이하의 문자 또는 숫자여야 합니다. ※ 현재의 비밀번호가 5회이상 연속으로 물리면 Key Token의 보안협은 자동으로 경입니다. 비밀번호 변경

그림 44. KeyToken 초기화 시작

vyToken Manager v2.0.0.0	
인인증서 관리 KeyToken 관리 www.keypair.co.kr	
보안토르이란? 물리적 보안 및 암호 연산 기능을 가진 칩을 내장하고 있어 해킹 동으로부터 공인인증서 유출을 방지하는 기능을 가진 안전성이 강화된 휴대용 공인인증서 저장마체입니다. - 한국인터넷진흥원(KISA) 홈페이지 증에서 -	KeyToken 제품 정보 제조사 : Keypair 모델명 : KeyToken HSM H/W ver. : [1.0 명 문문 문
KeyToken은	F/W ver. : 1.0 비료 법정 Net ken Manager 또한원 KeyToken의 보안집이 조기확됩니다. KeyToken HSM의 구성도
KeyToken 앱 설치 : 0R코드 (안드로이드용)	보안토콘과 백업영역 안의 모든 데이터는 삭제됩니다. 단, KeyToken MSD의 microSD나 KeyToken USB의 USB 메모리 안의 데이터는 삭제되지 않습니다. 계속하시겠습니까? 5 에(^) 아니요(N)
	모든 데이터가 초기행됩니다. ※ KeyToken MSD의 microSDLI KeyToken USB의 USB 해요리 안의 데이터는 삭제되지 않습니다. 초기화 비밀번호가 5회이상 연속으로 들리면 KeyToken의 보안함은 자동으로 잡깁니다. 비밀번호 변경

그림 45. KeyToken 초기화 확인

6 그림 46 화면에서 '예' 버튼을 눌러, 초기화함을 다시 확인합니다.

보안토길이ぞ서 관리 KeyToken 관리 www.keypair.co.kr 보안토길이관? 물리적 보안 및 암호 연산 기능을 가진 칩을 내경하고 있어 해킹 등으로부터 공인인증서 유출을 받지하는 기능을 가진 안전성이 강화된 휴대용 공인인증서 저장매채입니다. - 한국인터넷진흥왕(KISA) 홈페이지 중에서 -	KeyToken 加善 登旦 加乏사: KeyDair 모델명: KeyToken HSM H/W ver.: 1.0
KeyToken은 NFC를 지원하는 스마트폰에서도 공인인증서를 안전하게 사용할 수 있는 보안트릴입니다. KeyToken HSM/MSD/USB 등의 모델이 있습니다. KeyToken 앱 설치 : OR코드 (안드로이드용)	F/W ver, : 1.0 관 예업 여 S/N : 0001101000000001 Token Manager Key Token HSM의 구성도 소 보안토콘과 백업영역 안의 모든 공인인증서들이 삭제됩니다. 정말로 계속하시겠습니까? 6 이(*) 아니요(*)
NUSB 포트에 KeyToken HSM0! 연결되어 있습니다.	※ Kay Tolen 보안협 (보안물급 + 백업영역) 안약 오든 데이터가 초기합됩니다. ※ Key Tolen K00의 microSDLF Key Token USB의 USB 해도리 안약 데이터는 삭제되지 않습니다. 초기참 비밀번호가 5회이상 연속으로 즐리면 Key Token K00의 microSDLF Key Token USB의 초기참 비밀번호 반경 프로그램 중료

그림 46. KeyToken 초기화 재확인

7 ユ	림 47 화면에서	'확인'버튼	을 눌러, Key	yToken 초기화를	완료합니다.
------------	-----------	--------	-----------	-------------	--------

보안토큰이란?	KeyToken 제품 정보	
물리적 보안 및 암호 연산 기능을 가진 첩을 내장하고 있어 해킹 등으로부터 공인인증서 유출을 방지하는 기능을 가진 안전성이 강화된 휴대용 공인인증서 저장매세입니다. - 한국인터넷진홍원(KISA) 홈페이지 중에서 -	제조사 : Keypair 모델명 : KeyToken HSM H/W ver, : 1.0	
KeyToken은	F/W ver, : 1.0	K2 4889 NFC
NFC를 지원하는 스마트폰에서도	S/N: 0001101000000001	보안침
공인인증서를 안전하게 사용할 수 있는 보안토큰입니다. KeyToken HSM/MSD/USB 등의 모델이 있습니다.	KeyToken Manager	KeyToken HSM의 구성도
	-	
KeyToken 앱 설치 : QR코드 (안드로이드용)	() KeyToken의 보안칩을 성공적으로 초기화하였습니다.	— KeyToken 비밀번호 변경
	7	현재의 비밀번호 :
	확인	변경할 비밀번호 :
- お御絵語が	alson de la concessa	비밀번호 확인 :
178-21403	※ KeyToken 보안칩 (보안토큰 + 백업영역) 안의 모든 데이터가 초기화됩니다.	※ 비밀번호는 8자이상 16자이하의 문자 또는 숫자여야 합니다.
	※ KeyToken MSD의 microSDLF KeyToken USB의 USB 메모리 안의 데이터는 삭제되지 않습니다.	※ 현재의 비밀번호가 5회미상 연속으로 틀리면 KeyToken의 보안첩은 자동으로 잠깁니다.
	*71×1	비만비승 비경
		necz co

그림 47. KeyToken 초기화 완료

4. KeyToken 비밀번호 변경

보안상 모든 비밀번호는 주기적으로 변경하는 것이 좋습니다. 마찬가지로 KeyToken 비밀 번호도 주기적으로 변경할 것을 권장합니다.

이 절에서는 KeyToken Manager로 KeyToken 비밀번호를 변경하는 과정을 예를 들어서 설명합니다.

먼저, PC의 USB 포트에 KeyToken을 연결한 후, 다음의 단계를 시작합니다.

- 1
 III장 3절의 'KeyToken 초기화'에서 [1] 단계를 실행하여, KeyToken Manager를 실행

 시킵니다.
- 2 III장 3절의 'KeyToken 초기화'에서 [2] 단계를 실행하여, 'KeyToken 관리' 탭을 선택 합니다.

f[®]Keypair

3 그림 48 화면에서 현재의 KeyToken 비밀번호와 변경할 KeyToken 비밀번호를 입력 합니다.

보안토큰이란?	KeyToken 제품 정보	
물리적 보안 및 암호 연산 가능을 가진 칩을 내장하고 있어 해킹 등으로부터 공인인증서 유출을 방지하는 기능을 가진 안전성이 강화된 휴대용 공인인증서 저장매체입니다. - 한국인터넷진종원(KISA) 홈페이지 중에서 -	제조사: Keypair 모델명 : KeyToken HSM H/W ver, : [1,0	
KeyToken은	F/W ver, : 1,0	
NFC를 지원하는 스마트폰에서도 공인인증서를 안전하게 사용할 수 있는 보안토큰입니다. KouTakea HSM MSD (USB 등의 모텍에 있습니다.	S/N : 0001101000000001 사용상태 : 정상적으로 동작중입니다.	또만의 KeyToken HSM의 구성도
	Key Token 초기화 라벨(선택 사학): 네일번호 : 네일번호 확인 : 또 Key Token 보안쉽 (보안토르 + 백업영역) 안의 모든 데이터가 초가회됩니다. ※ Key Token 사망의 배대야 SDLF Key Token USB의 USB 배모리 안의 데이터는 삭제되지 않습니다. 초기화	KeyToken 비밀번호 변경 현재의 비밀번호 : 변경할 비밀번호 비밀번호 확인 : ※ 비밀번호는 8자이상 16자이하의 문자 또는 숫자여이 합니다. ※ 현재의 비밀번호가 5최이상 연속으로 들리면 KeyToken의 보안컵은 자동으로 잠깁니다. 비밀번호 변경

그림 48. KeyToken 비밀번호 입력

4 그림 49 화면에서 '비밀번호 변경' 버튼을 누릅니다.

보안토큰이란?	KeyToken 제품 정보	
물리적 보안 및 암호 연산 기능을 가진 첩을 내장하고 있어 해킹 등으로부터 공인인증서 유용을 방지하는 기능을 가진 안전성이 강화된 휴대용 공인인증서 저장매체입니다. - 한국인터넷진홍원(KISA) 홈페이지 중에서 -	제조사: Keypair 모열명: KeyToken HSM H/W ver,: [1.0	
- KeyToken은 NFC를 지원하는 스마트폰에서도 공인인용서를 안전하게 사용할 수 있는 보안토클입니다. KeyToken HSM/MSD/USB 등의 모델이 있습니다.	F/W ver, : 1.0 S/N : 000110100000001 사용상태 : 전상적으로 동작중입니다.	KeyToken HSM의 구성도
KeyToken 앱 설치 : OR코드 (안드로이드용)	KeyToken 초기화 라벨(선택사합): 미정업 HSM 사용할 비밀번호: 비밀번호 확인: 또 KeyToken 보안철 (보안트클 + 백업영역) 안의 모든 (40161가 초가화됩니다. 또 KeyToken MSD의 microSDL KeyToken USB의 USB 해모리 안의 (40161는 석제되지 않습니다. 초기화	Key Token 비밀번호 변경 현재의 비밀번호 : 변경할 비밀번호 : 비밀번호 환경 : ····································

그림 49. KeyToken 비밀번호 변경 시작

f[®]Keypair

5 그림 50 화면에서 '확인' 버튼을 눌러, KeyToken 비밀번호 변경을 완료합니다.

보안토큰이란?	KeyToken 제품 정보	
물리적 보안 및 암호 연산 가능을 가진 첩을 내장하고 있어 해킹 등으로부터 공인인증서 유출을 방지하는 가능을 가진 안전성이 강화된 휴대용 공인인증서 저장매세입니다. - 한국인터넷진공원(KISA) 홈페이지 중에서 -	제조사: Keypair 모델명 : KeyToken HSM H/W ver,: [1,0	
KeyToken은	F/W ver, : 1.0	
NFC를 지원하는 스마트폰에서도 공이이즈 내로 아저희에 내용한 수 있는 법안트코인데트	S/N: 0001101000000001	±₩8
S전전등서를 전전하게 사용을 두 있는 모전도관입니다. KeyToken HSM/MSD/USB 등의 모델이 있습니다.	KeyToken Manager	KeyToken HSM의 구성도
KeyToken 앱 설치 : QR코드 (안드로이드용)	() KeyToken 비밀번호가 성공적으로 변경되었습니다.	F KeyToken 비밀번호 변경
	5	현재의 비밀번호 : ●●●●●●●●
「国務法国」	확인	변경할 비밀번호 : ●●●●●●●●●
「大学なない」	uses ac . j	비밀번호 확인 : ●●●●●●●●
7782294223	※ KeyToken 보안첩 (보안토큰 + 백업영역) 안의 모든 데이터가 초기화됩니다.	※ 비밀번호는 8자이상 16자이하의 문자 또는 숫자여야 합니다.
	※ KeyToken MSD의 microSDLi KeyToken USB의 USB 메모리 안의 데이터는 삭제되지 않습니다.	※ 현재의 비밀번호가 5회미상 연속으로 들리면 KevToken의 보안찮은 자동으로 장갑니다.
	* 71 ±1	
	22.71.21	01202 08

그림 50. KeyToken 비밀번호 변경 완료

5. 키페어 홈페이지 연결

KeyToken Manager에서 'www.keypair.co.kr' 탭을 선택하면, 키페어 홈페이지로 연결됩니다.

KeyToken Manager v2.0.0.0						×
공인인증서 관리 KeyToken 관리 www.keypair.co.kr						
f ìKeypair	* 회사소개	* 보안 하드웨어	* 보안 소프트웨어	 ↓다운로드 	* 고객센터	
Information Security Hardware & Software						н
NOTICE & NEWS more+ [간급] 아려 공지의 조치 02-04 [간급] keyToken 01-17 면처기업 확인을 받았습니다 01-02 매업장재산현에 소개되었습니 10-26 키페어 홈페이지를 오른하였 10-23		L		TikeyTokenUS	BG BB	
× USB 포트에 KeyToken HSMOI 연결되어 있습니다.				Anarchan Color	로그램 중료	-

그림 51. 키페어 홈페이지 연결

IV. KeyToken 사용하기

KeyToken은 금융 및 공공기관 홈페이지와 연동하여 공인인증서 로그인, 공인인증서 발급, 공인인증서 갱신 등에 사용할 수 있습니다.

1. 공인인증서 로그인

KeyToken으로 금융 및 공공기관 홈페이지에 로그인하는 과정은 기존의 이동식 디스크의 공인인증서로 로그인하는 과정과 거의 동일합니다.

이 절에서는 인터넷뱅킹 가입자가 KeyToken으로 은행 홈페이지에 로그인하는 과정을 예를 들어서 설명합니다. 다른 금융 및 공공기관 홈페이지에서도 아래와 거의 동일한 과정으로 로그인할 수 있습니다.

먼저, PC의 USB 포트에 KeyToken을 연결한 후, 다음의 단계를 시작합니다.

- 1 그림 52 화면처럼 웹 브라우저 주소창에 은행 홈페이지 주소를 입력하여, 은행 홈페이지에 접속합니다.
- 2 그림 52 화면에서 '로그인'을 누릅니다.



그림 52. 은행 홈페이지 접속





그림 53. 공인인증서 로그인 시작

4 그림 54 화면에서 'Keypair KeyToken: 1.0.0.5'를 선택합니다.

		- • ×
🗲 🕣 🜃 https://obank.kbst 🔎 👻 🔒 K. 🖹 C	× ₩ MyKB_MyPage (개인화 ×	ñ * ¤
· ** 로그인 인터넷명칭 서비스들 이용하기	위한 로그인 개인 기업 전체서비스 =	<u>م</u>
	····································	E
공인인증서 로그인	아드 디스크 이용적 디스크 사장 또한 적 XecureHSM10000 구분 사용자 만료열 발급자 로그인	
공인인증서 로그: 인증서 자동 편 인증서발급/개발급 티행/	인증사 보기 인증사 보기 인증사 약지 인증사 삼호 인증사 삭제 환인 취소	
		÷

그림 54. KeyToken 선택

1°Keypair

5 그림 55 화면에서 KeyToken 비밀번호를 입력합니다.

6 그림 55 화면에서 '확인' 버튼을 눌러, 로그인합니다.

🗲 🔿 🖪 https://obianik.kbst 🔎 - 🔒 K. 🗟 C :	× ☑ MyK8_MyPage (개인화 ×	- □ × ↑★☆
* 초 로그인 인터넷뱅킹 서비스플 이용하기 위	한 로그인 개인 기업 전체서비스 - 준 전자 서명 작성	•
공인인증서 로그업	····································	Е
<mark>공인인증서 로그와</mark> 인종서 자동 때 인종서발급/매발급 티世/	인증서 보기 인증서 보기 인증서 찾기 도금 암호 (1977년 등 도금의 암호를 입력하세요. 인증서 삭제 5 6 확인 취소	
	💌 💊 🐄 🔷	×

그림 55. KeyToken 비밀번호 입력

7 그림 56 화면처럼 로그인된 화면을 확인합니다.



그림 56. 공인인증서 로그인 완료

- ※ 증권사 홈페이지에서 KeyToken을 처음으로 사용하는 경우, 그림 57과 같은 화면이 나타날 수 있습니다. 이 화면은 KeyToken을 보안토큰이 아닌 저장토큰으로 사용할 것인지 묻는 것으로 반드시 아래와 같이 '사용안함'으로 설정하셔야 합니다.
- 1 그림 57 화면에서 '이 저장장치에 대해서 다시 묻지 않음' 체크박스를 체크합니다.
- 2 그림 57 화면에서 '사용안함'을 누릅니다.



그림 57. 증권사에서 KeyToken 처음으로 사용하기

- ※ 만약, '사용(OK)'로 설정하였다면, 아래의 과정으로 반드시 '사용안함'으로 변경하시기 바랍니다.
- 1 그림 58 화면에서 윈도우의 '시작' 버튼을 누릅니다.



그림 58. 윈도우 시작 버튼 누르기

2 그림 59 화면의 '프로그램 및 파일 검색' 창에 'regedit'를 입력하고, 엔터키를 눌러 실행합니다.



그림 59. regedit 실행하기

3, 4그림 60 화면처럼 HKEY_CURRENT_USER/Software/AppDataLow/SignKorea/Configuration/pkiclient 밑에 USE_SMARTCARD 항목을 찾습니다.

1특 섬퓨터	이름	종류	데이터
HKEY_CLASSES_ROOT HKEY_CURRENT_USER	환(기본값) 한IC_INTERFACE	REG_SZ REG_SZ	(값 설정 안 됨) SKCommIC.dll
Console	IC_SERIALPORT_SCAN	REG_DWORD REG_DWORD	0x00000000 (0) 0x000000002 (2)
- EUDC - Identities	PCSC_READER_ALLOW PCSC_READER_DENY STATUS BAR ON	REG_SZ REG_SZ REG_DWORD	JAEIK CSR;SCT SPK2032;KDE Inc. SmartCard Rea AKS;Rainbow Technologies iKey;Samsung Wibro; 0x00000001 (1)
Reyboard Layout Network Printers	USE_DISKETTE	REG_SZ REG_SZ	t t
Software AhnLab AppDataLow	USE_KEYSAFER USE_NETWORK A	REG_SZ REG_SZ REG_SZ	t f
SignKorea Configuration pkiclient Error Report		REG_SZ	t
A cromenta			

그림 60. USE_SMARTCARD 항목 찾기

7



5,6 그림 61 화면에서 값 데이터에 'f'를 입력하고,'확인' 버튼을 누릅니다.

그림 61. USE_SMARTCARD 값 데이터 변경하기

그림 62 화면에서 USE_SMARTCARD의 데이터가 'f'로 변경된 것을 확인합니다.



그림 62. USE_SMARTCARD 값 데이터 변경 확인하기

2. 공인인증서 발급

KeyToken은 공인인증서를 안전하게 저장하고 또 안전하게 사용하기 위한 보안토큰으로, 한국인터넷진흥원(KISA)의 구현적합성 평가를 받은 제품입니다.

공인인증서는 이동식 디스크나 하드 디스크 또는 보안토큰으로 발급받을 수 있습니다. 하지만, 이동식 디스크나 하드 디스크로 발급받을 경우, 공인인증서가 파일 형태로 저장 되어 쉽게 복사가 가능하기 때문에 해킹에 매우 취약합니다. 그래서, 한국인터넷진흥원 (KISA)도 공인인증서를 저장하기 위한 전용 보안 장치인 보안토큰으로 발급받을 것을 권장하고 있습니다.

보안토큰으로 공인인증서를 발급받으면 공인인증서의 외부유출이 원천적으로 방지되어 공인인증서를 가장 안전하게 사용할 수 있습니다.

보안토큰으로 공인인증서를 발급받는 과정은 기존의 이동식 디스크로 공인인증서를 발급 받는 과정과 거의 동일하며, 자세한 과정은 거래하시는 금융기관 홈페이지를 참조하시기 바랍니다.

※ 참고로, 보안토큰 안에 저장되어 있는 공인인증서는 이동식 디스크나 하드 디스크로 복사되지 않음에 주의하시기 바랍니다. 가족간에 공인인증서를 공유하는 경우처럼 공인인증서의 복사가 필요한 경우라면, 이동식 디스크로 공인인증서를 발급받은 후, 이동식 디스크의 공인인증서를 보안토큰으로 복사하여 보안토큰을 사용하시고, 공인 인증서가 저장되어 있는 이동식 디스크는 사용하지 마시고 안전한 곳에 보관하시기 바랍니다.

3. 공인인증서 갱신

KeyToken은 공인인증서를 안전하게 저장하고 또 안전하게 사용하기 위한 보안토큰으로, 한국인터넷진흥원(KISA)의 구현적합성 평가를 받은 제품입니다.

보안토큰 안에 저장되어 있는 공인인증서를 갱신하는 과정은 기존의 이동식 디스크 안에 저장되어 있는 공인인증서를 갱신하는 과정과 거의 동일하며, 자세한 과정은 거래하시는 금융기관 홈페이지를 참조하시기 바랍니다.

※ 참고로, 보안토큰 안에 저장되어 있는 공인인증서는 이동식 디스크나 하드 디스크로 복사되지 않음에 주의하시기 바랍니다. 만약 원본 공인인증서를 이동식 디스크에 보관하고 있고 사본 공인인증서를 보안토큰 안에서 사용하고 있다면, 반드시 원본 공인인증서를 갱신한 후에 갱신된 원본 공인인증서를 다시 보안토큰으로 복사하여 사용하시기 바랍니다.

V. FAQ

Q. KeyToken이란 무엇인가요?

A. KeyToken은 공인인증서를 안전하게 저장하고 또 안전하게 사용하기 위한 보안토큰 으로, 한국인터넷진흥원(KISA)이 KeyToken의 보안토큰에 대한 구현적합성을 평가하고 인증한 제품입니다. PC에서는 USB로 연결하여, 스마트폰에서는 NFC로 연결하여 사용 하실 수 있습니다.

Q. KeyToken은 왜 사용해야 하나요?

A. 최근 공인인증서 유출로 인한 금융사고들이 증가하고 있습니다. 하드 디스크에 저장
 되어 있는 공인인증서는 해킹으로 쉽게 유출될 수 있으며, 이동식 디스크에 저장되어
 있는 공인인증서는 이동식 디스크의 분실로 인해 쉽게 유출될 수 있습니다.

KeyToken은 물리적 보안 및 암호연산기능을 가진 보안칩을 내장하여 공인인증서의 외부유출을 원천적으로 방지하며, KeyToken 비밀번호가 연속으로 5회이상 틀리면 KeyToken이 자동으로 잠겨버려 분실시에도 안전합니다. 그래서, 한국인터넷진흥원 (KISA)은 보안토큰의 사용을 강력히 권장하고 있습니다.

Q. KeyToken을 사용할 수 있는 곳은 어디인가요?

A. PC 환경에서는 은행, 증권사, 보험사, 신용카드사 등 대부분의 금융기관과 전자민원, 국세청 등 대부분의 공공기관 홈페이지에서 KeyToken을 사용하실 수 있습니다. 다만, 드물게 보안토큰을 지원하지 않는 사이트들이 존재합니다. 이 경우, KeyToken의 백업 영역에 보관되어 있는 공인인증서를 이동식 디스크로 복사하여 사용할 수 있습니다.

NFC를 지원하는 스마트폰 환경에서는 아직 KeyToken의 보안토큰 기능은 사용하실 수 없지만, KeyToken의 백업영역 기능을 이용하여 대부분의 금융앱에서 현재의 방식보다 안전하게 공인인증서를 사용하실 수 있습니다. 자세한 내용은 'KeyToken App Manual' 을 참조하시기 바랍니다.

Q. 이동식 디스크에서 사용하던 공인인증서를 KeyToken에서도 사용할 수 있나요?

A. 네, 사용하실 수 있습니다. 이동식 디스크에 저장되어 있는 공인인증서를 KeyToken
 으로 복사하여 사용하시면 됩니다.

Q. 공인인증서를 KeyToken에 저장했는데, 다른 매체로 복사할 수 없나요?

A. KeyToken은 보안토큰 기능과 백업영역 기능이 있습니다. KeyToken의 보안토큰에 저장 되어 있는 공인인증서는 다른 매체로 복사하실 수 없습니다. 하지만, KeyToken의 백업 영역에 보관되어 있는 공인인증서는 다른 매체로 복사하실 수 있습니다.

Q. KeyToken 비밀번호를 잊어버렸습니다. 어떻게 해야 하나요?

A. 죄송합니다만, 현재 KeyToken의 보안토큰과 백업영역 안에 저장되어 있는 공인인증서 들은 더 이상 사용하실 수 없습니다. KeyToken 비밀번호가 연속으로 5회이상 틀리면 KeyToken은 자동으로 잠겨버립니다. KeyToken을 초기화하시고, 공인인증서를 새로 발급받으시거나 다시 복사해 넣으셔야 합니다.

Q. KeyToken 구동 프로그램을 다운로드 받아 실행하려고 하는 데, "KeyTokenSetup.exe 은(는) 일반적으로 다운로드되는 파일이 아니며, 컴퓨터를 손상시킬 수 있습니다."는 경고 메시지가 나옵니다. 어떻게 해야 하나요?

A. Internet Explorer 9 이상에서 SmartScreen 필터가 활성화되어 있는 경우, 위의 경고 메시지가 나타날 수 있습니다. 이는 마이크로소프트사의 SmartScreen 필터의 정책인 '해당 프로그램을 상당한 수의 다른 Internet Explorer 사용자가 다운로드한 프로그램 목록'에 없기 때문으로, 걱정하지 마시고 설치하시면 됩니다.

Q. KeyToken을 PC의 USB 포트에 연결하였는 데, "장치 드라이버 소프트웨어가 제대로 설치되지 않았습니다."는 경고 메시지가 나옵니다. 어떻게 해야 하나요?

A. KeyToken 구동 프로그램이 정상적으로 설치되지 않은 경우, 위의 경고 메시지가 나올
 수 있습니다. KeyToken 구동 프로그램을 다시 설치하시기 바랍니다.

[Blank Page]